

中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料

設定解説資料 （LANSCOPE エンドポイントマネージャー クラウド版 ～Android～）

Ver1.1 (2024.03)

本書は、総務省の調査研究事業により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）

総務省 サイバーセキュリティ統括官室

Email telework-security@ml.soumu.go.jp

URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

1 はじめに	3
2 チェックリスト項目に対応する設定作業一覧	4
3 管理者向け設定作業	5
3-1 チェックリスト 2-4 への対応	5
3-1-1 アプリケーションの制限	5
3-2 チェックリスト 5-1 への対応	8
3-2-1 メーカーサポートの確認	8
3-3 チェックリスト 7-2 への対応	12
3-3-1 タイムゾーン変更の検知設定	12
3-4 チェックリスト 8-1 への対応	16
3-4-1 端末位置の把握	16
3-5 チェックリスト 8-2 への対応	19
3-5-1 リモートロック・リモートワイプの実行	19
3-6 チェックリスト 9-1 への対応	22
3-6-1 Android 端末のパスワードポリシー設定	22
3-7 チェックリスト 9-2 への対応	24
3-7-1 エンドポイントマネージャーのログインパスワード変更	24
3-8 チェックリスト 10-1 への対応	25
3-8-1 エンドポイントマネージャーの管理者権限の付与	25
3-9 チェックリスト 10-2 への対応	31
3-9-1 エンドポイントマネージャーのログインパスワード強度	31
3-10 チェックリスト 10-3 への対応	31
3-10-1 エンドポイントマネージャーの管理者権限の管理	31

1 はじめに

（ア）本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目について、LANSCOPE エンドポイントマネージャー クラウド版（以下エンドポイントマネージャー）を利用した具体的な作業内容の解説をすることで、管理者が利用時に実施すべき作業の理解を助けることを目的としています。

（イ）前提条件

本製品のライセンス形態はすべて有償で「ライト A」「ライト B」「ベーシック」が存在します。利用するライセンス種類により使用可能な機能が異なります。**本資料では「ライト A」ライセンスの利用を前提としております。**（2023 年 11 月 7 日現在）

（ウ）本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者（これらに準ずる役割を担っている方を含みます）を対象として、その方々がチェックリスト項目の具体的な対策を把握できるよう、第 2 章ではチェックリスト項目に紐づけて解説内容と解説ページを記載しています。本書では第 3 章にて管理者向けに、設定手順や注意事項を記載しています。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責事項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および注意事項の解説が記載されたページを記載しています。
3 管理者向け設定作業	対象のチェックリスト項目に対する管理者向けの設定手順や注意事項を解説しています。

（エ）免責事項

本資料は現状有姿でご利用者に提供するものであり、明示であると黙示であるとを問わず、正確性、商品性、有用性、ご利用者様の特定の目的に対する適合性を含むその他の保証を一切行うものではありません。本資料に掲載されている情報は、2023 年 11 月 7 日時点の各製品の操作画面を基に作成しており、その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。本製品をご利用者様の業務環境で利用する際には、本資料に掲載している設定により業務環境システムに影響がないかをご利用者様の責任にて確認の上、実施するようにしてください。本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

2 チェックリスト項目に対応する設定作業一覧

本書で解説しているチェックリスト項目、対応する設定作業解説および注意事項が記載されているページは下記のとおりです。

表 2. チェックリスト項目と管理者向け設定作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
2-4 マルウェア対策 スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	<ul style="list-style-type: none"> ・ アプリケーションの制限 	P.5
5-1 脆弱性管理 テレワーク端末にはメーカーサポートが終了した OS やアプリケーションを利用しないよう周知する。	<ul style="list-style-type: none"> ・ メーカーサポートの確認 	P.8
7-2 インシデント対応・ログ管理 テレワーク端末と接続先の各システムの時刻を同期させる。	<ul style="list-style-type: none"> ・ タイムゾーン変更の検知設定 	P.12
8-1 データ保護 スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	<ul style="list-style-type: none"> ・ 端末位置の把握 	P.16
8-2 データ保護 テレワーク端末の紛失時に備えて MDM 等を導入し、リモートからのデータ消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用する。	<ul style="list-style-type: none"> ・ リモートロック・リモートワイプの実行 	P.19
9-1 アカウント・認証管理 テレワーク端末のログインアカウントや、テレワークで利用する各システムのパスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。	<ul style="list-style-type: none"> ・ Android 端末のパスワードポリシー設定 	P.22
9-2 アカウント・認証管理 テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。	<ul style="list-style-type: none"> ・ エンドポイントマネージャーのログインパスワード変更 	P.24
10-1 特権管理 テレワーク端末やテレワークで利用する各システムの管理者権限は、業務上必要な最小限の人に付与する。	<ul style="list-style-type: none"> ・ エンドポイントマネージャーの管理者権限の付与 	P.25
10-2 特権管理 テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用する。	<ul style="list-style-type: none"> ・ エンドポイントマネージャーのログインパスワード 	P.31
10-3 特権管理 テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用する。	<ul style="list-style-type: none"> ・ エンドポイントマネージャーの管理者権限の管理 	P.31

3 管理者向け設定作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第2部に記載されているチェックリスト項目のうち、本製品の管理者が実施すべき対策の設定手順や注意事項を記載します。

3-1 チェックリスト 2-4 への対応

3-1-1 アプリケーションの制限

LANSCOPE では、Android 端末に対し、アプリのインストールに関わる制限を詳細に設定することはできませんが、「新規アプリのインストール禁止」や「インストール済アプリの起動禁止」の設定を行うことができます。下記の手順は必須の設定ではありませんが、新規アプリのインストール禁止の設定方法及びインストール済みアプリの起動制限の設定方法を参考として記載しています。

新規インストールアプリの禁止設定

【手順①】

ホーム画面から「ルール」をクリックし、「アプリ設定」をクリック後、画面上部の Android を選択します。

アプリ名	デベロッパー	カテゴリー	パッケージ名	レベル
(S)Edy!au	楽天Edy株式会社	ショッピング	jp.edy.edyapp	不許可
(S)Feel on!	L is B corporation	ソーシャルネットワーク	com.lisb.feelon	許可
(S)LISMO Book Store			com.kddl.android.lismobook...	必須
(S)LISMO WAVE			com.kddl.android.lismowave	許可
(S)LiveShare	Cooliris	ソーシャルネットワーク	com.cooliris.app.liveshare	許可
(S)Photo Air			com.kddl.photoair	不許可
(S)picplz	picplz.com	写真	com.picplz.rangefinder	許可
(S)Sockets LIVE	Sockets Inc.	ソーシャルネットワーク	com.sockets.live	必須

【手順②】

グループのツリー表示で設定するグループを選択し、「変更」をクリックします。

【手順③】

「新規インストールアプリ」を「禁止」に設定し、「保存」をクリックします。

新規アプリに割り当てるアプリ管理レベル

LANSCOPE で管理しているいずれかのデバイスにアプリがインストールされた時に、以下で設定したアプリ管理レベルが自動的に割り当てられます。

新規インストールアプリ

禁止

必須

許可

未設定

不許可

禁止

プリインストールアプリ

許可

キャンセル 保存

インストール済アプリ毎の利用禁止設定

【手順①】

ホーム画面から「ルール」をクリックし、「アプリ設定」をクリック後、画面上部の Android を選択します。

LANSCOPE リスト レシビ モニター レポート ログ **ルール** 設定管理者

デバイス設定 Apple サービス設定 Android Enterprise 設定 記録メディア制御 配信設定 **アプリ設定**

iOS **Android** Windows macOS

継承 の設定を使用しています

アプリ共通の管理レベル初期設定 変更

新規インストールアプリ 禁止
プリインストールアプリ 許可

アプリ毎の管理レベル設定

すべて すべて 検索

アプリ管理レベルの追加

<input type="checkbox"/>	アプリ名	デベロッパー	カテゴリー	パッケージ名	レベル	インストール状況
<input type="checkbox"/>	(S)Edy!au	楽天Edy株式会社	ショッピング	jp.edy.edyapp	不許可	インストール済み
<input type="checkbox"/>	(S)Feel on!	L is B corporation	ソーシャルネットワーク	com.lisb.feelon	許可	インストール済み
<input type="checkbox"/>	(S)LISMO Book Store			com.kddi.android.lismobook...	必須	インストール済み
<input type="checkbox"/>	(S)LISMO WAVE			com.kddi.android.lismowave	許可	インストール済み
<input type="checkbox"/>	(S)LiveShare	Cooliris	ソーシャルネットワーク	com.cooliris.app.liveshare	許可	インストール済み
<input type="checkbox"/>	(S)Photo Air			com.kddi.photoair	不許可	インストール済み
<input type="checkbox"/>	(S)picplz	picplz.com	写真	com.picplz.rangefinder	許可	インストール済み
<input type="checkbox"/>	(S)Sockets LIVE	Sockets Inc.	ソーシャルネットワーク	com.sockets.live	必須	インストール済み

【手順②】

グループのツリー表示で設定するグループを選択し、利用を禁止したいアプリにチェックを入れ、「管理レベルの変更」をクリックします。

ネットワーク全体

- 総務課
- 人事課
- 営業部
- システム部
- サポートセンター
- 運輸部
- 検証用

Android

の設定を使用しています

アプリ共通の管理レベル初期設定

新規インストールアプリ 禁止

プリインストールアプリ 許可

アプリ毎の管理レベル設定

すべて

検索

1 件を選択中

インストール済みのアプリは削除できません

管理レベルの変更

アプリ名	デベロッパー	カテゴリ	パッケージ名	レベル	インストール状況
(S)EdyJau	楽天Edy株式会社	ショッピング	jp.edy.edyapp	不許可	インストール済み
(S)Feel on!	L is B corporation	ソーシャルネットワーク	com.lisb.feelon	許可	インストール済み
(S)LISMO Book Store			com.kddi.android.lismobook...	必須	インストール済み
(S)LISMO WAVE			com.kddi.android.lismowave	許可	インストール済み
(S)LiveShare	Cooliris	ソーシャルネットワーク	com.cooliris.app.liveshare	許可	インストール済み
(S)Photo Air			com.kddi.photoair	不許可	インストール済み
<input checked="" type="checkbox"/> (S)picplz	picplz.com	写真	com.picplz.rangefinder	許可	インストール済み
(S)Sockets LIVE	Sockets Inc.	ソーシャルネットワーク	com.sockets.live	必須	インストール済み

【手順③】

「禁止」にチェックを入れ、「設定」をクリックします。

アプリの管理レベルの設定

☐ 必須
アプリがインストールされていないデバイスを抽出することができます。

☐ 許可
デバイスへのインストールやアプリの起動を許可します。

☐ 未設定
管理レベルが未設定である状態にします。

☐ 不許可
アプリの起動やインストールが行われたデバイスを抽出することができます。

☒ 禁止
アプリの起動を禁止することができます。

キャンセル

設定

3-2 チェックリスト 5-1 への対応

3-2-1 メーカーサポートの確認

利用する端末の OS やアプリケーションは、製品提供元からサポートのあるバージョンを利用します。サポート切れの OS やアプリケーションを使用していると不具合や脆弱性が修正されないため、不正アクセスの起点となってしまう恐れがあり、セキュリティ上のリスクとなります。利用している Android バージョンのサポート期間や今後の更新予定などについては製品提供元（※）に確認してください。

※ 主要 3 キャリアの製品アップデート情報サイト

NTT ドコモ：https://www.nttdocomo.co.jp/support/product_update/

au：https://www.au.com/information/notice_mobile/update/

ソフトバンク：<https://www.softbank.jp/mobile/info/personal/software/>

ここでは、LANSCOPE を利用して、端末の OS バージョンを確認する方法を記載します。

OS バージョン確認方法

【手順①】

ホーム画面から「リスト」-「デバイス」をクリックし、エンドポイントマネージャーに登録されているデバイスリストが表示から対象のデバイスをクリックします。



	↑ ↓	デバイスグループ	使用人名	OSタイプ	OSバージョン	電話番号
<input type="checkbox"/>	1	総務課	■■■■■	Android	9	090xxxxxxx
<input type="checkbox"/>	2	総務課	■■■■■	Android	10	090xxxxxxx
<input type="checkbox"/>	3	営業1課	■■■■■	iOS	14.4	080xxxxxxx
<input type="checkbox"/>	4	人事課	■■■■■	Android	11	080xxxxxxx

【手順②】

画面左にある「デバイス情報」をクリックします。システムの欄に表示されている「OS バージョン」より確認できます。



指定した Android のバージョン範囲外の検知

【手順①】

ホーム画面から「レシピ」を選択し、「レシピ一覧」から「レシピの追加」をクリックします。



【手順②】

任意のレシピ名を入力後、「トリガーを選択」をクリックし、「Android」のタブから、「Android のバージョンが指定した範囲外になっている」を選択します。

The left screenshot shows the '新しいレシピを作成' (Create New Recipe) screen. The 'レシピ名' (Recipe Name) field is highlighted in red. Below it, the 'トリガーを選択' (Select Trigger) button is highlighted in red. The right screenshot shows the 'トリガーを選択してください' (Please select a trigger) screen. The 'Android' tab is selected, and the trigger 'Android のバージョンが指定した範囲外になっている' (Android version is outside the specified range) is highlighted in red.

【手順③】

OS バージョンの範囲を指定し、「レシピを実行する対象の絞り込み」を設定し、「アクション追加」をクリックします。
（下記記載例では OS のバージョンを 10 から 12 までとし、デバイスグループをレシピの実行対象として設定）

The screenshot shows the '新しいレシピを作成' (Create New Recipe) screen. The 'OSバージョン (下限)' (OS Version (Lower Limit)) is set to 10 and 'OSバージョン (上限)' (OS Version (Upper Limit)) is set to 12. The 'デバイスグループ' (Device Group) is set to '人事課 (1台)' (Personnel Department (1 device)). The 'アクション追加' (Add Action) button is highlighted in red.

【手順④】

次に、アクションを選択します。ここでは「アラートに設定する」を選択し、アラートレベル（危険/注意/警告なし）を「注意」に設定し、保存します。

アクションを選択してください

	IOS	Android	Windows	macOS
管理者にメールでお知らせする	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定プロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
指定アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
指定プロビジョニングプロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
指定 VPP アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
メッセージを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
アンケートを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
アラートに設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
アラートレポートを送信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定プロファイルを取り除く	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

アラートレベルを選択してください

アラートレベル*

注意

設定

新しいレシピを作成

レシピ名*

バージョン情報

レシピのトリガーを選択

トリガー*

Androidのバージョンが指定した範囲外になっている

OSバージョン（下版）*

10

OSバージョン（上版）*

12

レシピを実行する対象の絞り込み

デバイスグループ（1 件）

選択

人事課（1 台）

デバイス（0 台）

選択

1 台のデバイスが対象になっています。 ※ 対象デバイスが多い場合、レシピの実行に時間がかかる可能性があります。

実行するアクション

アクション追加

アラートに設定する

アラートレベル*

注意

編集

保存

【手順⑤】

ホーム画面から「リスト」を選択し、「アラート」から、対象のアラートを確認します。

アラート対象の端末がある場合は、右側に対象端末が表示され、対象端末をクリックするとその端末の詳細画面が開きます。

警告レベル	アラート	アラート台数
危険	未稼働期間が指定された期間を超過している	5 台
注意	空き容量が不足している	2 台
危険	パスコードロックの設定がオフになっている	4 台
危険	デバイスの設定がリモート操作の実行条件を満たしていない	3 台
注意	SIMカードが抜き差しされた	2 台
注意	Androidのバージョンが指定した範囲外になっている	2 台
注意	もうすぐリース切れになる	1 台
危険	SDカードが抜き差しされた	1 台
危険	指定したアプリが実行された	1 台
危険	新しくアプリがインストールされた	1 台
危険	位置情報が取得されない設定になっている	1 台
注意	LANSCOPE Client のバージョンが最新になっていない	1 台

3-3 チェックリスト 7-2 への対応

3-3-1 タイムゾーン変更の検知設定

この項目では、端末のタイムゾーンの変更を検知するように設定を行います。端末のタイムゾーンの変更により日付や時刻がずれると、セキュリティインシデント発生時のログの調査の際に、発生事象の時系列が追えなくなるリスクがあります。こうしたリスクを低減するためにタイムゾーンが変更されたら検知するようにし、利用者に設定を戻すように促すことができます。

【手順①】

ホーム画面から「レシピ」を選択し、「レシピ一覧」から「レシピの追加」をクリックします。

【手順②】

任意のレシピ名を入力し、「トリガーを選択」をクリック後、「操作ログ情報」を選択します。選択後、「Android」から、「タイムゾーンが変更された」を選択します。

新しいレシピを作成

レシピ名*
タイムゾーン変更通知

レシピのトリガーを選択 トリガー選択

トリガー*
-

レシピを実行する対象の絞り込み

デバイスグループ (0 件)
選択

デバイス (0 台)
選択

実行するアクション アクション追加

トリガーを選択してください

すべて iOS **Android** Windows macOS

デバイス情報

☒ 操作ログ情報

位置情報

任意のタイミング

	iOS	Android	Windows	macOS
デバイスが不正に改造されている(root化)	×	○	×	×
Androidのバージョンが指定した範囲外になっている	×	○	×	×
SIMカードが抜き差しされた	○	○	○	×
SDカードが抜き差しされた	×	○	×	×
デバイスの設定がリモート操作の実行条件を満たしていない	×	○	○	×
もうすぐリース切れになる	○	○	○	○
ログが取得されない設定になっている	×	○	×	×
空き容量が不足している	○	○	○	○
<input checked="" type="checkbox"/> タイムゾーンが変更された	×	○	×	×
位置情報が取得されない設定になっている	×	○	○	×

【手順③】

「レシピを実行する対象の絞り込み」を設定し、「アクション追加」をクリックします。

新しいレシピを作成

レシピ名*
タイムゾーン変更通知

レシピのトリガーを選択 トリガー選択

トリガー*
タイムゾーンが変更された

レシピを実行する対象の絞り込み

デバイスグループ (1 件)
選択

人事課 (1 台) ×

デバイス (0 台)
選択

1台のデバイスが対象になっています。 ※ 対象デバイスが多い場合、レシピの実行に時間がかかる可能性があります。

実行するアクション アクション追加

【手順④】

アクションを選択します。ここでは「アラートに設定する」を選択し、アラートレベル（危険/注意/警告なし）を「注意」で設定し、保存します。

アクションを選択してください

	IOS	Android	Windows	macOS
管理者にメールでお知らせする	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定プロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
指定アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
指定プロビジョニングプロファイルを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
指定 VPP アプリを配信する	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
メッセージを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
アンケートを配信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
アラートに設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
アラートレポートを送信する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
指定プロファイルを取り除く	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

アラートレベルを選択してください

アラートレベル*

注意

確定

新しいレシピを作成

レシピ名*

タイムゾーン変更通知

レシピのトリガーを選択

トリガー*

タイムゾーンが変更された

トリガー選択

レシピを実行する対象の絞り込み

デバイスグループ (1 件)

選択

人事課 (1 台)

デバイス (0 台)

選択

1 台のデバイスが対象になっています。 ※ 対象デバイスが多い場合、レシピの実行に時間がかかる可能性があります。

実行するアクション

アクション追加

アラートに設定する

アラートレベル*

注意

編集

保存

【手順⑤】

ホーム画面から「リスト」を選択し、「アラート」から、対象のアラートを確認します。

アラート対象の端末がある場合は、右側に表示され、対象端末をクリックするとその端末の詳細画面が開きます。

警告レベル	アラート	アラート台数
危険	未稼働期間が指定された期間を超過している	5 台
注意	空き容量が不足している	2 台
危険	パスコードロックの設定がオフになっている	4 台
危険	デバイスの設定がリモート操作の実行条件を満たしていない	3 台
注意	SIMカードが抜き差しされた	2 台
注意	iOSのバージョンが指定した範囲外になっている	2 台
注意	もうすぐリース切れになる	1 台
危険	SDカードが抜き差しされた	1 台
危険	指定したアプリが実行された	1 台
危険	新しくアプリがインストールされた	1 台
危険	位置情報が取得されない設定になっている	1 台
注意	タイムゾーンが変更された	1 台

3-4 チェックリスト 8-1 への対応

3-4-1 端末位置の把握

端末の盗難・紛失があった場合に備え、端末の位置情報を検出できるように設定します。端末の位置情報を検出できるように設定することにより、**端末の盗難・紛失時に端末の位置を特定できる可能性が高まり、情報漏洩のリスクを低減することができます。**

端末の位置情報を取得するためには、端下記の手順を実施することに加えて、末側で位置情報を取得する設定を有効にしている必要があります。

位置情報の取得設定

【手順①】

ホーム画面「ルール」から「デバイス設定」を選択し、「基本設定」をクリックします。



画面左側のデバイスグループから設定を適用するデバイスグループをクリックします。「Android」をクリックし、右側の「作成」をクリックします。



【手順②】

位置情報ログ取得設定欄で、「取得する」にチェックを入れ、取得間隔を指定し、「保存」をクリックします。

「業務時間のみ取得する」を有効にした場合は、設定した業務時間内でのみ位置情報を取得します。

「高精度で取得されない設定になっているデバイスに警告する」設定や「省電力設定（振動を検知して移動中のみ情報を取得）」を有効にすることもできます。

共通 iOS Android Windows macOS

継承 の設定を使用しています キャンセル 保存

位置情報ログ取得設定

位置情報
☒ 取得する

取得間隔 *
 3分 ▼

業務時間のみ取得する
☒ 有効

高精度で取得されない設定になっているデバイスに警告する
☐ 有効

省電力設定（振動を検知して移動中のみ情報を取得）
☐ 有効

業務時間は、同画面の「共通」から「編集」で設定できます。

共通 iOS Android Windows macOS

継承 の設定を使用しています 作成 削除

メモ

メモ
 .

業務時間設定

開始時刻
 00:00

終了時刻
 23:59

タイムゾーン
 (UTC+09:00) 大阪、札幌、東京

業務曜日
 月 / 火 / 水 / 木 / 金

休日設定 ④
 設定しない

業務日設定
 設定しない

端末位置の確認方法

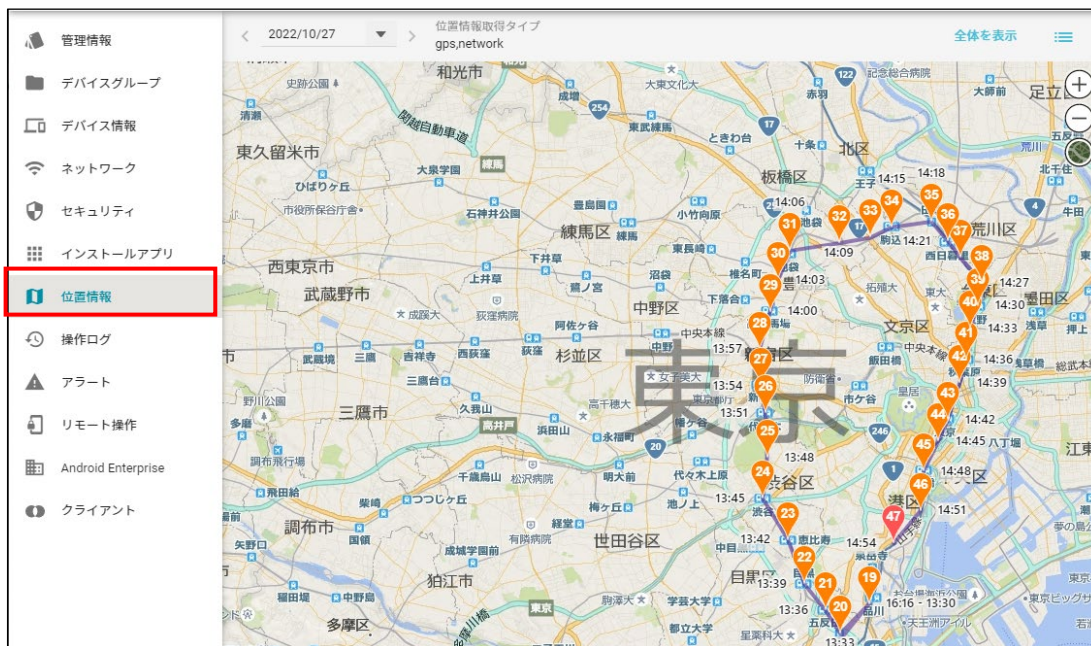
【手順①】

ホーム画面の「リスト」から、「デバイス」を選択し位置情報を確認したいデバイスをクリックします。



【手順②】

画面左にある「位置情報」を選択後、画面右側のマップにて現在の位置情報を確認できます。



3-5 チェックリスト 8-2 への対応

3-5-1 リモートロック・リモートワイプの実行

端末の紛失・盗難があった場合、遠隔操作で、端末のロック（リモートロック）や端末のデータを初期化（リモートワイプ）をすることができます。**紛失・盗難時に、端末のリモートロックやリモートワイプを行うことで、第三者に不正操作されるリスクを低減**します。

エンドポイントマネージャーからのリモートロック実行

例えば、端末を紛失し、一時的に利用不可としたい場合は、リモートロックを実行します。

【手順①】

ホーム画面から「リスト」を選択し、「デバイス」を選択します。


選択後、エンドポイントマネージャーに登録されているデバイスリストが表示されるので、対象のデバイスをクリックします。



	↑ ↓	デバイスグループ	使用人名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課	██████	Android	9
<input type="checkbox"/>	2	総務課	██████	Android	10
<input type="checkbox"/>	3	営業1課	██████	iOS	14.4
<input type="checkbox"/>	4	人事課	██████	Android	11
<input type="checkbox"/>	5	営業部	██████	Android	11

【手順②】

画面左にある「リモート操作」を選択後、「リモート操作を実行する」をクリックし、「リモートロックを実行」をクリックします。



管理情報

デバイスグループ

デバイス情報

ネットワーク

セキュリティ

インストールアプリ

位置情報

操作ログ

アラート

リモート操作

クライアント

リモート操作を実行する ▼

リモートロックを実行

リモートワイプを実行

リモートワイプ:成功

リモートワイプ:成功

リモートワイプ:成功

【手順③】

ロック解除用の任意のパスワードを入力して、「実行」をクリックします。これにより対象端末がロックされ使用できなくなります。Android11以降の端末では、パスワードの上書きはできません。パスワードの上書きをしたい場合は、Android Enterpriseを利用してデバイスを登録してください。（詳細：製品開発元のマニュアル「Android Enterprise 利用ガイド」を参照してください。）

リモートロックの実行

リモートロックを実行することで第三者による不正使用を防ぐことができます。

デバイスのロックを解除するパスワードは、入力したパスワードで再設定されます。

パスワード *

.....

パスワード(確認用) *

.....

キャンセル

実行

エンドポイントマネージャーからのリモートワイプ実行

【手順①】

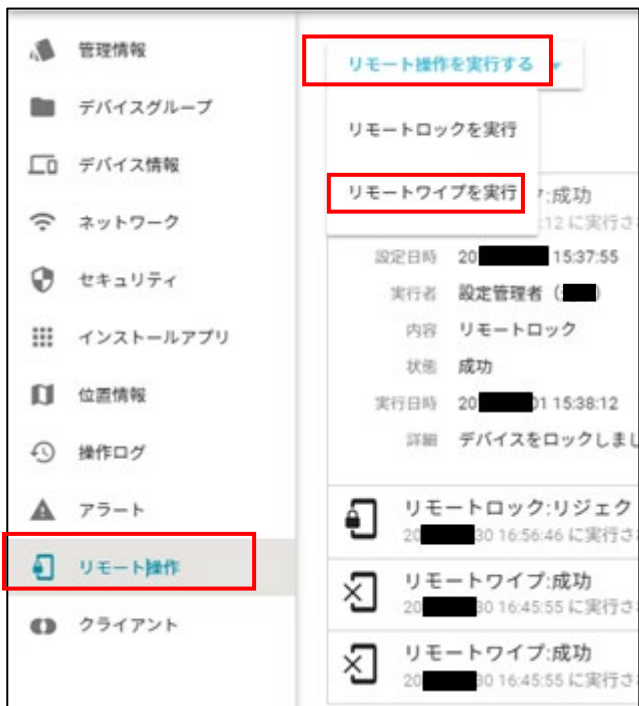
ホーム画面から「リスト」を選択し、「デバイス」を選択します。

選択後、エンドポイントマネージャーに登録されているデバイスリストが表示されるので、対象のデバイスをクリックします。

LANSCOPE					
リスト		レシビ	モニター	レポート	ログ
デバイス		アプリ	プロフィール	アラート	
ネットワーク全体		iOS	Android	Windows	macOS
デバイスの追加		インストール待ちデバイス			
<input type="checkbox"/>	↑ ↓	デバイスグループ	使用者名	OSタイプ	OSバージョン
<input type="checkbox"/>	1	総務課		Android	9
<input type="checkbox"/>	2	総務課		Android	10
<input type="checkbox"/>	3	営業1課		iOS	14.4
<input type="checkbox"/>	4	人事課		Android	11
<input type="checkbox"/>	5	営業部		Android	11

【手順②】

画面左にある「リモート操作」を選択後、「リモート操作を実行する」をクリックし、「リモートワイプを実行」をクリックします。



【手順③】

「リモートワイプの実行」画面でログインしている管理コンソールのアカウントのログインパスワードを入力し、「実行」をクリックします。これにより、対象端末のデータが初期化されます。

リモートワイプの実行

リモートワイプを実行することでデバイス内のすべてのデータを初期化できます。
 消去されたデータを復元することはできません。
 また、LANSCOPE の機能も使用できなくなります。

確認のためログインパスワードを入力してください。

ログインパスワード *

キャンセル

実行

3-6 チェックリスト 9-1 への対応

3-6-1 Android 端末のパスワードポリシー設定

管理者はパスワードポリシーを設定することにより、強度の高いパスワード設定をユーザーに要求できます。**これにより、強度の低いパスワードが使用されるリスクを低減することができます。**

パスワードポリシー設定

【注意事項】

Android10 以降の端末では、パスワードポリシーを適用できません。パスワードポリシーを適用したい場合は、[Android Enterprise](#) を利用してデバイスを登録して設定してください。（詳細：製品開発元のマニュアル「Android Enterprise 利用ガイド」を参照してください。）

【手順①】

ホーム画面から「ルール」から「デバイス設定」を選択し、「基本設定」をクリックします。



画面左側のデバイスグループから設定を適用するデバイスグループをクリックします。「Android」をクリックし、右側の「作成」をクリックします。



【手順②】

パスワードポリシー設定欄で、「パスワードポリシー」の「設定する」にチェックを入れ、ポリシーを設定し、「保存」をクリックします。

共通 iOS **Android** Windows macOS

継承 の設定を使用しています キャンセル **保存**

パスワードポリシー設定

⚠️ Android 10 以降のデバイスには適用されません。

パスワードポリシー
☒ 設定する

パスワードの最小文字数 *
8文字

使用しなければならない文字の種類 *
英字 + 数字

パスワードの有効期間
☒ 設定する
有効期間 (日) (1 ~ 730 日) *
90

パスワードの有効期限を事前に通知
☒ 通知する
通知日 *
3日前

以前使用したパスワードの再使用
☒ 禁止する
再使用禁止回数 *
2回

パスワード入力連続失敗によるデバイス初期化
☒ 初期化する
連続失敗回数 *
6回

デバイスのロック開始までの最大許容時間
☒ 設定する
最大許容時間 *
15秒

3-7 チェックリスト 9-2 への対応

3-7-1 エンドポイントマネージャーのログインパスワード変更

初期パスワードは、誰が把握しているかわからないので、速やかにパスワード要件を満たすものに変更することで、**悪意のある第三者から不正アクセスされるリスクを低減します。**

【手順①】

画面右上のログインアカウント隣の「▼」をクリックし、「パスワード変更」をクリックします。



【手順②】

現在のパスワードを入力し、新しいパスワードを入力後、「保存」をクリックします。




3-8 チェックリスト 10-1 への対応

3-8-1 エンドポイントマネージャーの管理者権限の付与

管理者権限を付与するユーザーを限定することで、本製品の設定変更をできるユーザーを必要最小限に抑え、**悪意のあるユーザーにより、意図しない設定変更が行われるリスクを低減することができます。**エンドポイントマネージャーを利用するユーザーを追加する場合は、利用できる機能権限（ロール）を制限したうえで追加することを推奨します。

エンドポイントマネージャーのデフォルトのロールは、全機能権限を持つシステム管理者のみとなります。以下の手順で、使用者の目的に応じたロールを作成してユーザーに割り当てることができます。

【手順①】

画面右上の「」をクリックし、「アカウント管理」をクリックします。



画面左側のメニューから「ロール」を選択し、「ロールの追加」をクリックします。



【手順②】

任意のロール名を入力し、付与したい機能権限を選択後、「追加」をクリックします。

以下の画面はロールとして、ログやアラートの確認のみができるロール「資産管理担当者用」を追加しています。

ロールの追加

ロール名 *

資産管理担当者用

すべてチェック

すべてはすす

機能権限

☐ アカウント管理ができる
☐ 運用設定ができる
☐ 資産情報を管理できる
☐ ファイル配信設定ができる (Windows)
☐ 資産系アラートが設定できる
☒ 資産系アラートを確認できる
☒ リモート操作の結果を通知できる
☐ 紛失モード・パスコードオフを実行できる
☐ 操作ログの取得設定ができる (iOS / Android)
☐ デバイスの PC 操作ログ設定ができる (Windows / macOS)
☒ 操作ログを確認できる (iOS / Android)
☒ 操作ログを確認できる (Windows / macOS)
☒ Windows / macOSの使用状況を確認できる
☒ レポートの集計設定ができる (Windows / macOS)
☐ 記録メディアの制御設定ができる (Windows / macOS)
☐ Windowsの更新設定ができる
☐ 操作系アラートが設定できる
☒ 操作系アラートを確認できる
☐ 位置情報の取得設定ができる
☒ 位置情報を確認できる
☐ リモートロックを実行できる
☐ リモートワイプを実行できる


キャンセル

追加

作成後、ロールの一覧に作成したロールが追加されます。

← システムメニュー		
<div> <div>アカウント管理</div> <div>アカウント</div> <div>ロール</div> <div>操作履歴</div> </div>	<div> <div>ロールの追加</div> <div> <input type="checkbox"/> システム管理者 <input checked="" type="checkbox"/> 資産管理担当者用 </div> </div>	
	<div> <div>アカウント管理ができる、運用設定ができる、資産情報を管理できる、ファイル配信設定ができる</div> <div>資産情報を管理できる、資産系アラートが設定できる、資産系アラートを確認できる</div> </div>	<div> <div>リフレッシュ</div> </div>

【手順③】

画面右上の「」をクリックし、「アカウント管理」をクリックします。



画面左側のメニューから「アカウント」をクリックし、「アカウントの追加」をクリックします。



【手順④】

「ロール」から「選択」をクリックします。

アカウントの追加

メールアドレス *

アカウントを識別するために使用されるメールアドレスです。このメールアドレスは変更できません。

表示名 *

営業

ロール *

選択

パスワード *

半角英字 1 文字以上、半角数字 1 文字以上を含んでください。

半角英数記号 8 ～ 15 文字以下で入力してください。

パスワードはメールアドレスと異なる値を入力してください。

パスワード確認用 *

ランダムなパスワードを自動で生成する

アクセス許可

▼ ☒ ネットワーク全体

☒ 総務課
 ☒ 人事部

▶ ☒ 営業部

▶ ☒ システム部

キャンセル

追加

「ロールを選択」画面で追加したロールをチェックし、「選択」をクリックします。

以下の画面は、【手順②】で追加した「資産管理担当者用」を選択しています。

※ 全権限を付与したいユーザーの場合は、「システム管理者」を選択します。

ロールを選択

×

1 件を選択中

選択

<input type="checkbox"/>	ロール名	機能権限
<input type="checkbox"/>	システム管理者	アカウント管理ができる, 運用設定ができる, 資産情報を管理できる, ファイル配信認
<input checked="" type="checkbox"/>	資産管理担当者用	資産情報を管理できる, 資産系アラートが設定できる, 資産系アラートを確認できる

【手順⑤】

「ロール」に選択したロールが追加されます。次に、メールアドレスや表示名、パスワードを入力し、アクセス許可するネットワークを選択後、「追加」をクリックします。これによりユーザーが使用できる権限を限定することができます。

アカウントの追加

メールアドレス *

アカウントを識別するために使用されるメールアドレスです。このメールアドレスは変更できません。

表示名 *

test

ロール *

選択

資産管理担当者用

パスワード *

.....

半角英字 1 文字以上、半角数字 1 文字以上を含んでください。
 半角英数記号 8 ～ 15 文字以下で入力してください。
 パスワードはメールアドレスと異なる値を入力してください。

パスワード確認用 *

.....

ランダムなパスワードを自動で生成する

アクセス許可

☒ ネットワーク全体

☒ 総務課
 ☒ 人事課

キャンセル

追加

ロールの変更

【手順①】

既存ユーザーをシステム管理者から変更する場合は、アカウント一覧から対象ユーザーをクリックし、「編集」をクリックします。



【手順②】

「選択」をクリックし、変更するロールにチェックを入れ、「選択」をクリックします。

設定管理者 () () - アカウント詳細

基本情報

アクセス許可

2 要素認証

アカウント (メールアドレス) ①

表示名 *

設定管理者 ()

ロール *

選択

システム管理者 (X)

作成日時

2017/12/05 17:01:27

キャンセル 保存

ロールを選択

X 1 件を選択中

選択

<input type="checkbox"/>	ロール名	機能権限
<input checked="" type="checkbox"/>	システム管理者	アカウント管理ができる, 運用設定ができる, 資産情報を管理できる, ファイル配信
<input type="checkbox"/>	資産管理担当者用	資産情報を管理できる, 資産系アラートが設定できる, 資産系アラートを確認できる

閉じる

「保存」をクリックします。これによりアカウントのロールが変更され、アカウントの権限が変更されます。

設定管理者 () () - アカウント詳細

基本情報

アクセス許可

2 要素認証

アカウント (メールアドレス) ①

表示名 *

設定管理者 ()

ロール *

選択

システム管理者 (X)

作成日時

2017/12/05 17:01:27

キャンセル 保存

閉じる

3-9 チェックリスト 10-2 への対応

3-9-1 エンドポイントマネージャーのログインパスワード強度

パスワード強度が弱いパスワードを使用した場合、パスワードが解読され、不正アクセスを受けるおそれがあります。そのため、適切なパスワードを設定することが重要です。設定するパスワードは「[中小企業等向けテレワークセキュリティの手引き](#)」の P.96 に記載の「パスワード強度」を参考に設定することを推奨します。

3-10 チェックリスト 10-3 への対応

3-10-1 エンドポイントマネージャーの管理者権限の管理

作業ミスによるシステムやデータへの悪影響を防ぐために、**一般ユーザーのアカウントを作成し、普段はそのアカウントを利用、管理者用アカウントの利用は最小限に留める**ことを推奨します。

【謝辞】

本設定解説資料の策定及び更新を行うにあたっては、エムオーテックス株式会社の関係各所の方々に多大なるご協力をいただきました。この場をお借りして深く御礼申し上げます。